論文賞受賞研究

「匿名通信のための情報量的に
安全な暗号化/認証技術」

「鍵漏洩耐性をもつ不正利用者追跡法」

2008.05.16
花岡 悟一郎
RCIS, AIST

はじめに

- 発表者の研究の大きな目的:「**高度に安全**」な暗号技術の追求
...「**高度に安全**」とは？
 - 数学的仮定の排除 (実現可能性重視)
 - より弱い数学的仮定 (実用性重視)
 - 秘密情報の漏洩への耐性

最近の成果の例

- 数学的仮定の排除

- Unconditionally Secure Group Authentication. *Comput. J.* 2006

The Wilkes Award
from
British Comp. Society

- 「印象に残った論文」の仮定

from
SCIS'08(非公式) 選択暗号文攻撃に対して証明可能
論文. SCIS'08予稿集, 2008.

- 秘密情報の漏洩への耐性

- Traitor Tracing Scheme Security
Exposure and its Application
IEICE Transactions 90-A

Best Paper Award
from
IEICE

「匿名通信のための情報量的に 安全な暗号化/認証技術」

- Unconditionally Secure Anonymous Encryption and Group Authentication. Hanaoka, Shikata, Imai. *Comput. J.* 49(3): 310-321, 2006.
- 匿名通信における、無条件に安全な秘匿/認証通信の理論的限界の解明と最適な実現方法の提示
- British Computer Society (英国) より、*The Wilkes Award (2006)* を受賞
 - 学術論文誌 *The Computer Journal* に掲載論文のうち、年間を通じて一件のみに授与される。

匿名通信路

匿名通信と情報量的安全性

匿名通信と情報量的安全性は両立が難しい！

この研究の成果

- 匿名通信と情報量的安全性を両立させるための条件を明確にした。
 - 鍵長, 暗号文長, etc...
- 実際に、この要件を満足する、最適な方式の存在を示した。

The Computer Journal

OXFORD JOURNALS CONTACT US MY BASKET MY ACCOUNT

the Computer Journal

ABOUT THIS JOURNAL CONTACT THIS JOURNAL SUBSCRIPTIONS CURRENT ISSUE ARCHIVE SEARCH

Institution: AIST Sign In as Personal Subscriber

[Oxford Journals](#) > [Mathematics & Physical Sciences](#) > Computer Journal

READ THIS JOURNAL

[View Current Issue \(Volume 51 Issue 3 May 2008\)](#)
[Advance Access](#)
[Browse the Archive](#)

The Computer Journal publishes research papers in a full range of subject areas, as well as regular feature articles and occasional themed issues to enable readers to easily access information outside their direct area of research. The journal provides a complete overview of developments in the field of Computer Science.

SEARCH THIS JOURNAL > [Advanced search](#)

FREE ONLINE ACCESS TO THE WINNING ARTICLE OF

the Computer Journal Wilkes Award 2007

RELATED JOURNALS

- > [ITNOW](#)
- > [IEICE - Transactions on](#)

READER SERVICES

- > [Special Issues](#)
- > [Free sample issue](#)

THE JOURNAL

- > [About this journal](#)
- > [Publishers' Books for Review](#)
- > [Rights & Permissions](#)
- > [Dispatch date of the next issue](#)
- > [The Wilkes Award](#)

Published on behalf of

- > [The British Computer Society](#)

Impact factor: 0.593

Editor-in-Chief
Professor E. Gelenbe
> [View full editorial board](#)

FOR AUTHORS

- > [Instructions to authors](#)

<http://comjnl.oxfordjournals.org/>

Maurice Wilkes

Recent changes
Direct Wikipedia
Redirect to Wikipedia

Search

Links here
Recent changes
Upload file
Special pages
Mobile version
Permanent link
History of this page

Sign in

Search

Help

Log out

Log in

My preferences

My watchlist

My contributions

My talk page

My user page

Sir Maurice Vincent Wilkes FRS (born [June 26, 1913](#) in [Dudley, Staffordshire, England](#)) is a [British computer scientist](#), credited with several important developments in [computing](#).

Wilkes studied at [St. John's College, Cambridge](#) from 1931 to 1934, continuing to complete a [Ph.D. in physics](#), on the topic of radio propagation of very long radio waves in the [ionosphere](#) in 1936. He was appointed to a junior faculty position of the [University of Cambridge](#) through which he was involved in the establishment of a computing laboratory.

Wilkes was called up for military service during [WWII](#) and worked on [radar](#) at the [Telecommunications Research Establishment](#) (TRE), and in [operational research](#).

In 1945, he was appointed as the second director of the [University of Cambridge Mathematical Laboratory](#) (later known as the [Computer Laboratory](#)).

The Cambridge laboratory initially had many different computing devices, including a [differential analyser](#). Wilkes obtained a copy of [John von Neumann's prepress description](#) of the

Maurice Vincent Wilkes

Born	June 26, 1913 (age 94) Dudley, Staffordshire
Nationality	British
Fields	Computer Science
Institutions	Telecommunications Research Establishment University of Cambridge Mathematical Laboratory British Computer Society Digital Equipment Corporation
Known for	Microprogramming
Notable awards	Turing Award

⋮

Wikipediaより引用

「鍵漏洩耐性をもつ 不正利用者追跡法」

- Traitor Tracing Scheme Secure against Adaptive Key Exposure and its Application to Anywhere TV Service. Ogawa, Hanaoka, Imai. *IEICE Transactions* 90-A(5): 1000-1011, 2007.
- 有料放送通信における、復号鍵の不正な二次配布者の追跡可能性と、秘密情報漏洩への耐性を同時に実現
- 電子情報通信学会(日本)より、**平成19年度論文賞**を受賞
 - 学術論文誌 *IEICE Trans. Fundamentals* に掲載論文のうち、年間を通じて三件のみに授与される。

有料放送通信

不正な二次配布者の存在もしくは不注意による鍵漏洩の問題

この研究の成果

- 次の二つの性質を満たす有料放送通信のための暗号方式の提案
 - 不正に二次配布された鍵から、その漏洩元となった利用者を特定可能。
 - ある時点における鍵情報が漏洩しても、それ以降における安全性は損なわれない。

過去の信学会論文賞受賞者

歴代論文賞受賞者一覧 - Microsoft Internet Explorer

アドレス http://www.ieice.org/jpn/about/rekidai/ronbunshou.html

電子情報通信学会
The Institute of Electronics, Information and Communi

歴代論文賞受賞者一

第15回 (昭和33年度) S34.5.16

選択性ビーム結合器 (Selective Beam Combining) (選定論文誌 33・6)

マイクロ波の見通内伝ばんのフェー

不要側帯波の悪影響を受けない鉱石

第16回 (昭和34年度) S35.5.14

周波数変調高感度受信方式 (選定論文誌 34・8) 森田正典・伊東祐弥

パラメトロンを用いた試作半電子交換機 (選定論文誌 34・3) 喜安春市・池野信一・勝沼進・福岡武治・花輪幸四郎

反射板による第2種無給電中継について (選定論文誌 34・5) 副島光積

第17回 (昭和35年度) S36.5.13

シルバーバンド・ダイオードの

進行波形パラメトリック増幅器 (選定論文誌 35・6)

逆根軌跡法によるトランジスタ

る波器のチェビシェフ近似理論 (選定論文誌 35・3) 渡部 和

第18回 (昭和36年度) S37.5.19

トンネル・ダイオードを用いたダウン・コンバータについて (選定論文誌 35・12) 家入勝吾

時間的並びに空間的旋回電界によるサイクロトロン波のパラメトリック増幅 (選定論文誌 36・6) 斎藤成文・見目正道

第48回 (平成3年度) H4.5.23

Location Problems on Undirected Flow Networks (英文論文誌 A 2・12) 田村 裕・仙石正和・篠田庄司・阿部武雄

An Urabe Type A Posteriori Stopping Criterion and a Globally Convergent Property of the Simplicial Approximate Homotopy Method (英文論文誌 A 3・6) 牧野光則・大石進一・柏木雅英・堀内和夫

任意の平面曲線上に符号を構成する方法 (論文誌 A 3・7) 神谷典史・三浦晋示・今井秀樹

第59回 (平成14年度) H15.5.28

Semantically Secure McEliece Public-Key Cryptosystem (論文誌 EA 14・1) 古原和邦・今井秀樹

「CDH仮定に基づく選択暗号文攻撃に対して証明可能安全な公開鍵暗号」

- CDH仮定に基づく選択暗号文攻撃に対して証明可能安全な公開鍵暗号. Hanaoka, Imai. SCIS'08 予稿集, 2008.
- 従来の方式よりも弱い仮定のみを用いて、選択暗号文攻撃への安全性を証明可能な公開鍵暗号方式を提案
- 国内研究会SCIS'08において、「印象に残った論文」部門(非公式 😊) 第一位に選ばれる。
 - 「聞き逃して残念な発表」部門でも第二位に選出。

簡単な背景: CCA安全性の仮定

弱 ← 強

SCIS2008投票結果

SCIS2008電子投票の結果報告 - Microsoft Internet Explorer

ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)

戻る 検索 お気に入り

アドレス(D) http://www.cs.dmu-tokai.ac.jp/scis2008/svis/result_rep.html

SCIS2008 電子投票 結果報告

SCIS2008電子投票に参加いただき、どうもありがとうございました。5名のミキサーによるシャッフルと復号が終了しましたので、集計結果をお知らせします。(ミックスネットの正当性証明データの公開及び検証は [こちら](#)から)

順位	「印象に残った論文」投票(48票)	「努力が伝わるプレゼン」投票(30票)	「聞き逃して残念な発表」投票(45票)
1	2F2-2「CDH仮定に基づく選択暗号文攻撃に対して証明可能安全な公開鍵暗号」、Goichiro Hanaoka 他、(6票) 3B1-4「署名付構造化文書への拡張 Bleichenbacher 攻撃の適用」、武仲正彦 他、(6票)	3D2-2「素因数分解専用ハードウェア開発プロジェクト」、下山武司 他、(5票)	3D2-2「素因数分解専用ハードウェア開発プロジェクト」、下山武司 他、(6票)
2	4D2-3「IDベース公開鍵暗号の応用」、境隆一、(5票)	3A3-2「実環境におけるAPOP攻撃実験」、佐藤玲 他、(4票)	2F2-1「放送暗号を用いたCCA安全な公開鍵暗号の新たな構成と一般化」、Goichiro Hanaoka 他、(5票) 2F2-2「CDH仮定に基づく選択暗号文攻撃に対して証明可能安全な公開鍵暗号」、Goichiro Hanaoka 他、(5票) 3F4-3「RSA Accumulator を用いた墨塗り署名方式について」、伊豆哲也 他、(5票)
3	2D1-4「国際量子暗号会議 UQC2007 の開催報告と今後の展開」、伊藤由季子 他、(4票)	2A1-2「AESの鍵スケジュールに対するフォールト攻撃」、高橋順子 他、(3票) 3B1-4「署名付構造化文書への拡張 Bleichenbacher 攻撃の適用」、武仲正彦 他、(3票)	2B2-5「ハッシュ関数に対する攻撃を考慮した電子署名の安全性」、沼山晃 他、(4票) 2E2-3「IDベース認証鍵交換の一方式」、小林鉄太郎 他、(4票) 2F1-4「二つのモデルの差を示す新たな暗号の実例」、西巻陵 他、(4票)